ARTICLE APPEARED
ON PAGE 4

THE CHRISTIAN SCIENCE MONITOR
6 December 1978

Cooley, John K.

CIA 3.01.7

How US, Soviets compete in electronic espionage

By John K. Cooley
Staff correspondent of
The Christian Science Monitor

Washington

Have Soviet spies operating in the United States compromised American electronic surveillance capacity in such a way as to interfere with future verification of their country's weapons systems under a new strategic arms-limitation treaty (SALT)?

The short answer to this, say senior US Defense Department officials, is that both SALT I and the draft SALT II agreement now under negotiation forbid such interference.

This has not stopped the Soviets from scrambling or encrypting the signals sent out by their own missile tests, making it more difficult for US monitoring devices to gather vital data on them.

Clues to Soviet priorities in their espionage efforts are found in the main spy cases uncovered in the US over the past year:

• Last month, former low-level Central Intelligence Agency (CIA) staffer William P. Kampiles was convicted in a Hammond, Indiana, court of selling a highly secret manual on the US KH-11 satellite surveillance system to a Soviet military attaché in Greece.

The Soviets, according to US agents, gave Mr. Kampiles $3,000 as "partial payment" for the manual, which described operation of the satellite as part of the "national technical means" of US intelligence collection. Satellites can be used for both communications and photo spying. They would play a central role in SALT verification.

Deputy CIA director for science and technology Leslie C. Dirks testified at the Kampiles trial that US national defense would be "seriously harmed" by the sale. However, another CIA official said not just one, but 17 out of 350 copies of the manual in question were missing and unaccounted for as of Nov. 1.

• In September, two former Soviet employees of the United Nations were convicted of conspiracy and espionage in a Newark, New Jersey, court. The Federal Bureau of Investigation in cooperation with US Navy intelligence officials caught the two Russians, who thought they were buying from US Navy personnal data on the Gurmman Tomcat F-14 fighter and the Navy's LAMPS anti-submarine warfare program. The latter is a system for gathering undersea intelligence electronically from light helicopters.

• In Miami on Nov. 10, 1977, an American and a West German were convicted of attempting to obtain for the USSR components of the US Navy's Tomahawk cruise missile.

Defense analysts think possession of the electronic missile ingredients that emit data signals, called telemetry, would enable the Soviets to reinforce their own "national technical means" of gathering data on US missile tests.

• In May, 1977, Christopher J. Boyce, a former employee of TRW Corporation's Space and Defense Systems, was convicted in Los Angeles on eight espionage counts for passing to the Soviets information on how intelligence data are transmitted between US ground stations and satellites in space.

• Two months before the Boyce conviction, two executives of another California defense electronics firm, I. I. Industries, were convicted of conspiring to export illegally other electronic equipment to the Soviets.

To prevent US surveillance, the Soviets have encrypted the telemetry of their SS-18 and SS-20 missiles, now deployed in both Eastern Europe and the northwestern Pacific.

Carter administration analysts, asked whether this tactic does not violate the SALT I agreement, usually reply that SALT I was never formally ratified. Electronic ciphers used by the Russians, they say privately, probably can be broken by the US, but the process is time-consuming and would delay verification of future missile tests under a SALT II agreement.